政府情報システムのためのセキュリティ評価制度（ISMAP）の見直しに向けての BSA ｜ザ・ソフトウェア・アライアンスからの提言

2021年12月7日

BSA| The Software Alliance[1]（BSA｜ザ・ソフトウェア・アライアンス、以下、「BSA」）は、内閣サイバーセキュリティセンター、経済産業省、総務省、および、デジタル庁（以下、「関係省庁」）が政府全体におけるクラウドサービスの導入を拡大し、公的部門において採用される可能性があるクラウドサービスの安全性を評価する「政府情報システムのためのセキュリティ評価制度」（以下、「ISMAP」）の改善に向けて取り組んでいることを高く評価します。

総論

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者 です。BSA の会員企業は、最先端のクラウドコンピューティング技術およびサービス提供で世界を牽引しており、各国政府が、ネットワークセキュリティやシステムの可用性を高めながら、その俊敏性、生産性、および革新性を向上することを支援しています。その経験に基づき、以下の提言を述べさせて頂くことで、クラウドサービスの円滑な導入という政府の目標の実現に貢献したいと考えております。

提言

現行の制度は、ISMAP クラウドサービスリストへの登録を希望するクラウドサービスプロバイダー（CSP）に、多大なコンプライアンス負荷と法外な費用を課すと同時に、制度の実施において、政府側の限りある人的資源も圧迫することから、今後の具体的な検討にあたっては、以下の点を考慮に入れて頂くことを我々は強く推奨します。

---

[1] BSA の活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, Zoomが会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

- **クラウドサービスの責任共有モデル[2]を認識すること。**安全なクラウド導入を成功させるには、クラウド利用者や調達者が職員を訓練し、クラウド環境で安全なアプリケーションを開発し、必要に応じて CSP が提供するツールや対策を自らの責任で利用し、セキュリティ・リスクを最小限に抑えることが求められている、ということを理解することが重要です。ISMAP に責任共有の原則を明確に盛り込むことにより、クラウドサービスのリスク管理をするための管理基準の策定と維持において、CSP と顧客との間とのクラウド運用に関しての異なる責任が認識されるようになります。また、自らが管理し、責任を負う環境の側面において、可視性の無い環境以外において、どの当事者が説明責任を負うのかを明確にすることができます。これにより、アクセス権を持たない顧客データやシステムに対して、セキュリティ要件や義務を CSP に課すということが回避され、不適切な義務を課せられた場合に、結果的にセキュリティやプライバシーに逆効果となる事態を避けることができます。

- **ISMAP をより柔軟に、実施しやすくすること。**様々なクラウドサービスのモデル(SaaS、IasS、PaaS)の特徴的な要件を考慮し、これらのサービス、また、導入された環境や組織に最も関連するリスクを管理するために最適化された必須のセキュリティ基準を定義することにより、現行の ISMAP を改善することができます。

- **反復的な監査手続を削減すること。**既に取得済みの国際規格と重複する管理基準の適用を免除することで、監査手続を簡素化し、人的資源を特定の限定的な基準に集中させることが可能となります。多くの CSP は、国際的に認定された認証機関から国際規格(ISMS-JISQ/ISO 27000 シリーズ)の認証を既に取得しています。それらを認め、過去の認証手続きで提供された証跡の再利用という反復的な手順と要件を排除することで、政府関係者を含む、全てのステークホルダーの負担を軽減することができます。また、これにより、日本で ISMS/ISO 認証を取得する企業が増え、そのような企業に国際的なビジネス・チャンスが広がり、政府に対して、より費用対効果の高いソリューションを提供するための競争が激化することにもなります。

- **第三者機関による国際的に認定された認証および監査結果を認めること。**ISMAP の関連する管理基準および要件に準拠している証拠の重複を削除することにで、非実用的で反復的な現地監査の必要性も減らすことができます。現地監査は、本目的以外では権限を持たない者による現場へのアクセスを要するため、データセンターを不必要な物理的セキュリティリスクにさらすことになります。

- **より具体的な監査ガイドラインを策定し、それらを国際的に認定された標準に合わせて位置付けること。**ISMAP の制度運営者、監査人、および CSP 間の管理基準の解釈の不一致は、CSP に非効率な手間、追加費用、および手続きの遅延を課すことになります。ISMAP 制度運営者と監査人による管理基準の解釈の違いにより、場合によっては、監査終了後に、CSP へ ISMAP 制度運営者から再監査依頼が繰り返されることがあります。

[2] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

- **ISMAP に登録する監査法人の数を増やすこと。**登録されている監査法人の数が限られているため、ISMAP で要求される監査手続を満たすための、現在また将来的な人的資源が不足しています。登録監査法人の数を現在の4法人から増やすことで、人材不足が解消され、監査法人間の公正な競争を促進することで、CSP に多様な選択肢を提供し、監査市場の効率化を図ることができます。また、ISMAP を持続可能な制度にするためには、クラウドサービスの IT 監査・認証要員を育成するための手続きを開発し、適切な人材を確保することが重要です。

- **頻度を減らした 監査スケジュールを設定すること。**毎年監査を実施するという ISMAP の要件とは対照的に、国際的なクラウド・セキュリティのベスト・プラクティスでは、一般的に三年に一度の監査を求めています。監査の頻度を減らすことで、CSP と政府の双方にとって不要なコストを削減することができます。毎年の監査では、CSP は事実上、連続した監査手続を実施することになり、常時、監査対応に追われることとなり、セキュリティ担当者の注意を不必要にそらし、他の重要な人材も流用することとなります。調達省庁側にとっても、毎年度の契約更新が求められることから、負荷が増すこととなります。

- **申請・登録の受付を、四半期ごとではなく、年間を通じて行うことができるようにすること。**現在、ISMAP 制度運営者は、ISMAP 認証・登録を希望する企業からの申請を四半期ごとに受け付けているため、ISMAP 登録を目指す CSP にとっては、三ヶ月以上の遅れが生じる可能性があります。このような遅延は、企業が貴重な調達機会に入札することを妨げ、企業には事業機会を、調達機関には対象となるクラウドサービスの恩恵を与えないことになります。年間を通して継続的に申請・登録を行うことで、ISMAP は急速に進化するクラウドの技術をより迅速に取り入れることができます。

上記の提言は、政府のサイバーセキュリティ戦略[3]とも合致しています。同戦略においては、「国は、政府情報システムのためのセキュリティ評価制度（ISMAP）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。クラウドサービスは外国企業により提供されているものも多いことから、グローバルな連携も進める」[4]と記されており、上記の ISMAP の改善を優先し、国際的なセキュリティ認証への認識を高めることは、日本において、セキュリティが保証されたクラウドサービスが普及することにつながります。

結論

上記の改善を実現するために、また、政府調達における選択肢を増やし、民間が提供するクラウド・サービスへの政府投資から、さらなる価値を生み出すために、グローバルに事業を展開する BSA 会員企業がどのように関係省庁と連携していけるかについて幅広い話し合いができることを期待しています。

---

[3] https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf

[4] 「サイバーセキュリティ戦略」（令和3年9月28日）、4.2.1（２）新たなサイバーセキュリティの担い手の協調、 p21